SPYWOLF

Security Audit Report

TESTNET

Completed on

November 24, 2022

MADE IN USA 🇺🇸

OVERVIEW

This audit has been prepared for **SPIN COIN** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

SPIN COIN

PROJECT DESCRIPTION

According to their whitepaper:

Spincoin is a tokenized game of roulette! Purchase of the token allows community members to have indirect exposure to one massive roulette spin a day – and one mega spin every Sunday! The community will vote on black or red in the Telegram chat till the poll is closed off every day at 5:30 PM EST. At 6PM EST the SPIN OF THE DAY will take place. ALL proceeds from the spin will go into buybacks until the next daily spin

Release Date: Presale starts in November, 2022

Category: Gamble

CONTRACT INFO

Token Name
SPINCOIN

Symbol
SPIN

Contract Address
NOT DEPLOYED

Network
Binance Smart Chain
NOT DEPLOYED

Language
Solidity

Deployment Date
N/A

Verified?
N/A

Total Supply
1,000,000,000,000,000

Status
Not deployed

TAXES

Buy Tax
9%

Sell Tax
9%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

CURRENT STATS

(As of November 24, 2022)

Liquidity

Not added yet

Burn

No burnt tokens

Status:

Not Launched!

MaxSellTxAmount

0.25% of total supply

DEX

PancakeSwap

LP Address(es)

Liquidity not added yet

TOKEN TRANSFERS STATS

Transfer Count	Contract not deployed yet
Uniq Senders	Contract not deployed yet
Uniq Receivers	Contract not deployed yet
Total Amount	Contract not deployed yet
Median Transfer Amount	Contract not deployed yet
Average Transfer Amount	Contract not deployed yet
First transfer date	Contract not deployed yet
Last transfer date	Contract not deployed yet
Days token transferred	Contract not deployed yet

SMART CONTRACT STATS

Calls Count	Contract not deployed yet
External calls	Contract not deployed yet
Internal calls	Contract not deployed yet
Transactions count	Contract not deployed yet
Uniq Callers	Contract not deployed yet
Days contract called	Contract not deployed yet
Last transaction time	Contract not deployed yet
Created	Contract not deployed yet
Create TX	Contract not deployed yet
Creator	Contract not deployed yet

FEATURED WALLETS

Owner address	Assigned at contract deployment
Treasury wallet	0x5d254A6127262E0e2D908118835dE21d7237167F
Ops wallet	0x8B32F6D68440c4cB04B8362fD17f0B21ef5b2801
LP address	**Liquidity not added yet**

TOP 3 UNLOCKED WALLETS

1 N/A

2 N/A

3 N/A

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ High Risk

Owner can initiate openTrading function once, however there is no limitation for 'blocks' input which sets the buy and sell taxes to 39% for the set period of time.

```
function openTrading(uint256 blocks) external onlyOwner {
    require(!tradingOpen, "Trading is already open");
    swapEnabled = true;
    cooldownEnabled = true;
    maxSellAmount = _tSupply.mul(25).div(10000);
    _swapTokensAtAmount = _tSupply.mul(25).div(100000);
    tradingOpen = true;
    tradingOpenBlock = block.number;
    _blocksToBlacklist = blocks;
    emit OpenTrading(tradingOpenBlock, _blocksToBlacklist);
}

function _tokenTransfer(address sender, address recipient, uint256 amount, bool takeFee, bool isSell) internal {
.....................
else amount = _takeFees(sender, amount, isSell);
.....................
}

function _takeFees(address sender, uint256 amount, bool isSell) internal returns (uint256) {
if(tradingOpenBlock + _blocksToBlacklist >= block.number) _setBot();
.....................
}

function _setBot() internal {
    _treasuryFee = 399;
    _opsFee = 399;
    _totalFees = _treasuryFee.add(_opsFee);
}
```

- Recommendation:
  - Set reasonable upper limit to the ‘blocks’ input.

FOUND THREATS

⚠ High Risk

Owner can blacklist address, making it impossible to sell.
If liquidity pair is blacklisted this will make it impossible to sell.

```
function setBlacklisted(address[] memory accounts, bool exempt) external onlyOwner {
    for (uint i = 0; i < accounts.length; i++) {
        if(accounts[i] != _pancakeSwapV2Pair) _isBlacklisted[accounts[i]] = exempt;
    }
}

function _transfer(address from, address to, uint256 amount) override internal {
.....................
if (from != owner() && to != owner() && to != ZERO && to != DEAD && !_swapping) {
require(!_isBlacklisted[from] && !_isBlacklisted[to]);
.....................
}
```

- Recommendation:
  - Considered as good practice is liquidity pair, router address and token's address(this) to be excluded from such restrictions.

FOUND THREATS

⚠ High Risk

Owner can set buy/sell fees up to 30%.
Combined buy+sell=60%.

```
function setBuyFee(uint256 newBuyTreasuryFee, uint256 newBuyOpsFee) external onlyOwner {
    require(newBuyTreasuryFee.add(newBuyOpsFee) <= 300, "Must keep buy taxes below 30%");
    buyTreasuryFee = newBuyTreasuryFee;
    buyOpsFee = newBuyOpsFee;
    emit SetBuyFee(buyTreasuryFee, buyOpsFee);
}

function setSellFee(uint256 newSellTreasuryFee, uint256 newSellOpsFee) external onlyOwner {
    require(newSellTreasuryFee.add(newSellOpsFee) <= 300, "Must keep sell taxes below 30%");
    sellTreasuryFee = newSellTreasuryFee;
    sellOpsFee = newSellOpsFee;
    emit SetSellFee(sellTreasuryFee, sellOpsFee);
}
```

- Recommendation:
  - Considered as good practice is buy and sell fees combined not to exceed 25%.

Informational

Owner can set cooldown blocks up to 10 before each transaction.

```
function setCooldownBlocks(uint256 blocks) external onlyOwner {
    require(blocks <= 10, "Invalid blocks count.");
    _cooldownBlocks = blocks;
}
```

Owner can exclude address from fees and max transaction limit.

```
function setExcludedFromFees(address[] memory accounts, bool isEx) external onlyOwner {
    for (uint i = 0; i < accounts.length; i++) _isExcludedFromFees[accounts[i]] = isEx;
}

function setExcludeFromMaxTransaction(address[] memory accounts, bool isEx) external onlyOwner {
    for (uint i = 0; i < accounts.length; i++) _isExcludedMaxTransactionAmount[accounts[i]] = isEx;
}
```

Owner can set max sell transaction amount but cannot lower it than 0.1% of total supply.

```
function setMaxSellAmount(uint256 maxSell) external onlyOwner {
    require(maxSell >= (totalSupply().mul(1).div(1000)), "Max sell amount cannot be lower than 0.1% total supply.");
    maxSellAmount = maxSell;
    emit SetMaxSellAmount(maxSellAmount);
}

function _transfer(address from, address to, uint256 amount) override internal {
.....................
if (to == _pancakeSwapV2Pair && from != address(_pancakeSwapV2Router) && !_isExcludedMaxTransactionAmount[from]) {
require(amount <= maxSellAmount, "Transfer amount exceeds the maxSellAmount.");
shouldSwap = true;
}
.....................
}
```

Informational

Owner can withdraw any tokens from the contract.

```
function withdrawStuckBNB() external onlyOwner {
    bool success;
    (success,) = address(msg.sender).call{value: address(this).balance}("");
}

function withdrawStuckTokens(address tkn) external onlyOwner {
    require(tkn != address(this), "Cannot withdraw this token");
    require(IERC20(tkn).balanceOf(address(this)) > 0, "No tokens");
    uint amount = IERC20(tkn).balanceOf(address(this));
    IERC20(tkn).transfer(msg.sender, amount);
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

SPIN COIN

GOOD PRACTICES FOUND

- ✔ The owner cannot mint new tokens after deployment
- ✔ The smart contract utilizes "SafeMath" to prevent overflows

⚠️Currently there is no information about the initial tokens distribution based on the project's whitepaper and/or website.

THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

⚠️ No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.

WEBSITE

Website URL
https://www.spincoin.network/

Domain Registry
https://www.godaddy.com

Domain Expiration
Expires on 2023-11-22

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

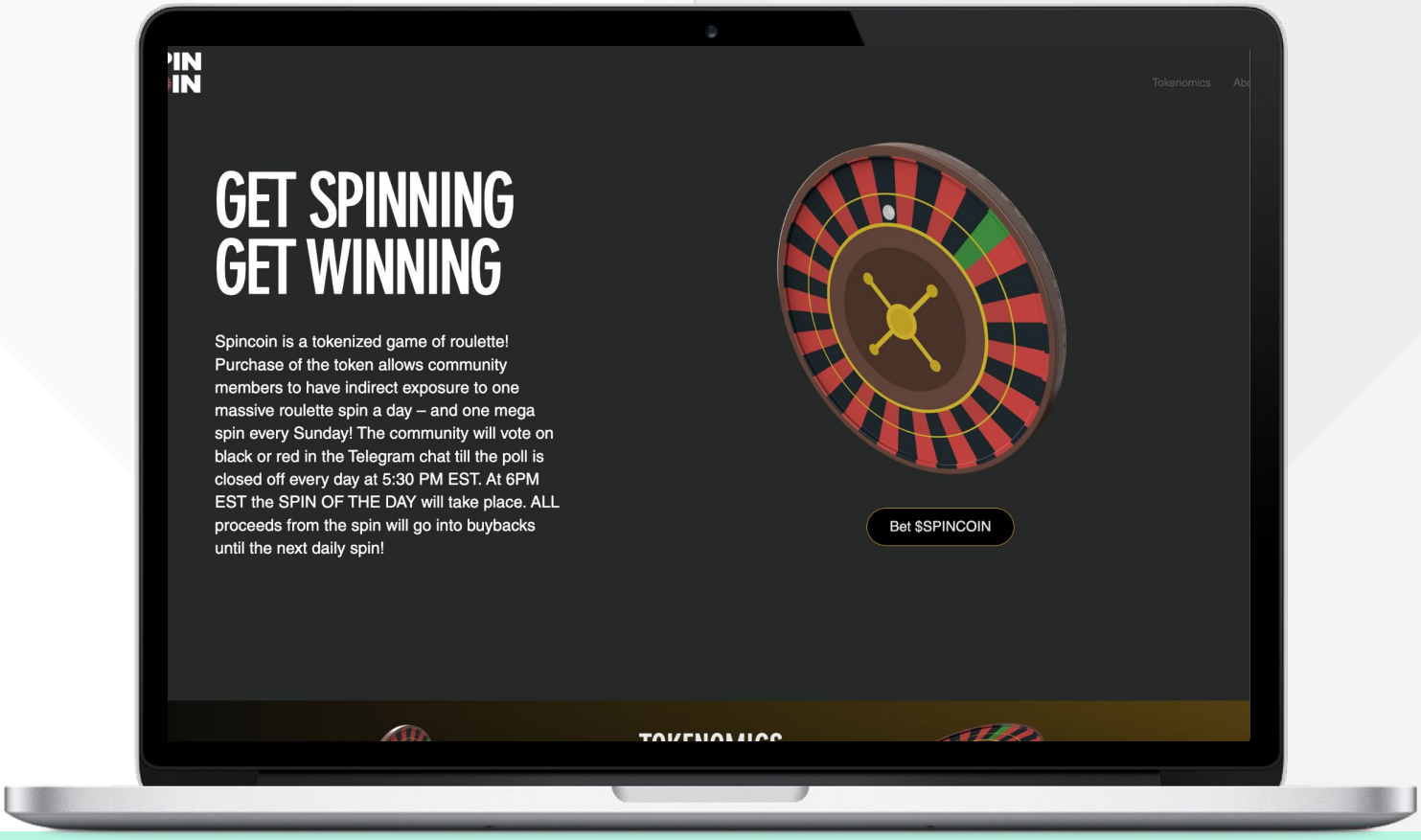
Design
Single page design, appropriate color scheme and graphics.

Content
The information helps new investors understand what the product does but there is not much information. No grammar mistakes found.

Whitepaper
⚠️ No whitepaper.

Roadmap
⚠️ No.

Mobile-friendly?
Yes



spincoin.network

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

⚠️ The project have none social media presence

Twitter

- Not available

Discord

- Not available

Telegram

- Not available

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 150 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

SPYWOLF.NETWORK

@SPYWOLFNETWORK

@SPYWOLFOFFICIAL

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.